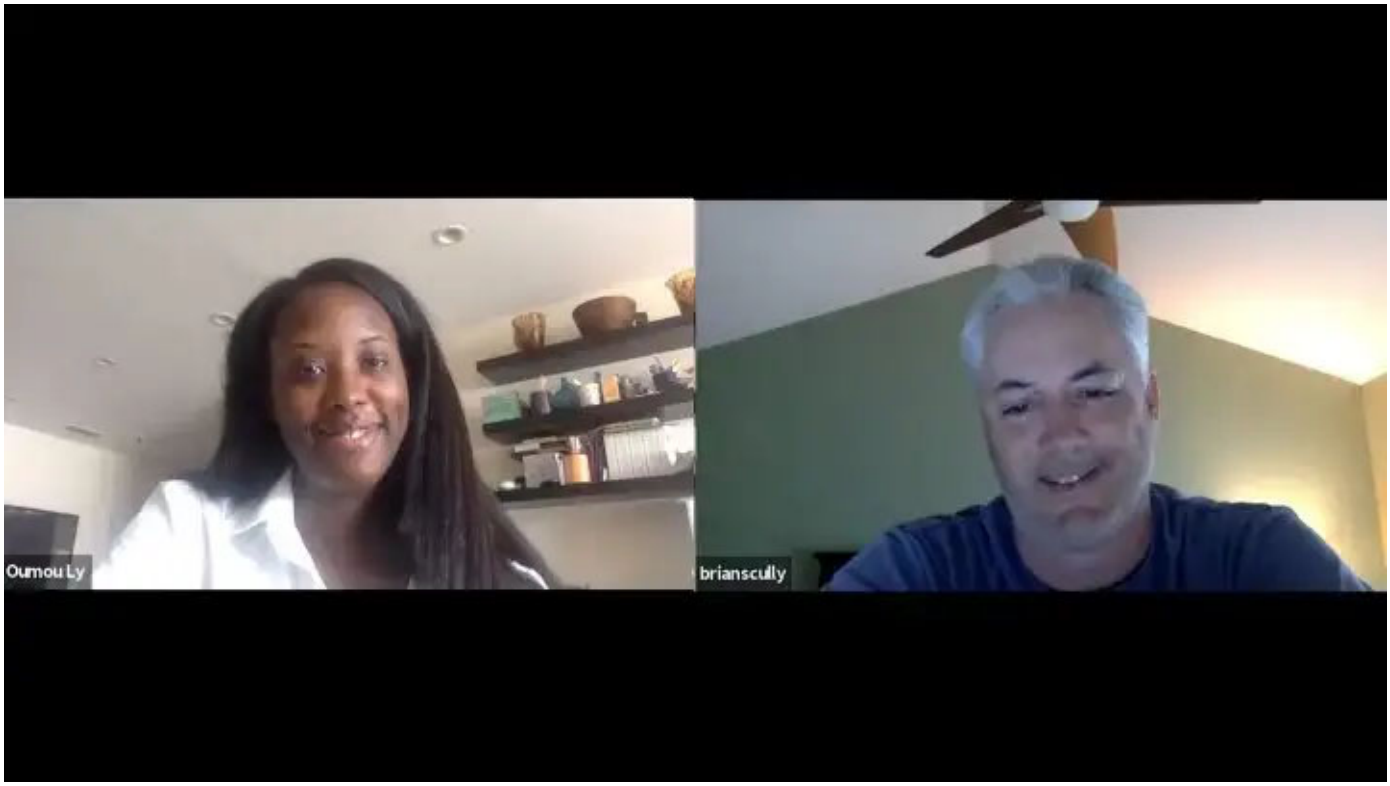
Berkman Klein Center Follow
Jun 18, 2020 · 12 min read · Listen

EXHIBIT 49

Save

# The Breakdown: Brian Scully on government response to disinformation

## Disinformation and the U.S. 2020 presidential election, COVID-19




Oumou Ly interviews Brian Scully for an episode of The Breakdown. Photo: Lydia Rosenberg

Amidst concerns of health disinformation in the current pandemic, scholars and practitioners have kept an eye on the 2020 presidential election in the United States.

In this episode of *The Breakdown*, BKC staff fellow Oumou Ly interviews Brian Scully of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and a 2019–20 member of the Assembly professional fellowship cohort to discuss how DHS is responding to the pandemic and preparing for the 2020 election, and what Scully has learned from the 2016 election.

Watch The Breakdown from the Berkman Klein Center

*Below is a transcript of the interview. It has been lightly edited for clarity.*

**Oumou Ly (OL): Welcome to The Breakdown. My name is Oumou. I am a staff fellow on the Berkman Klein Center Assembly: Disinformation program. Our topic for today is the upcoming November election. With us today, we have Brian Scully from the Department of Homeland Security, [who] will introduce himself.**

**Brian Scully (BS):** Currently, I run the DHS Countering Foreign Influence Task Force, which is in the Cybersecurity and Infrastructure Security Agency [CISA]. I've been doing that for about two years now.

**OL: Awesome. So, the election, with all that is going on in the country right now, seems to be a little bit of a third thought behind COVID and ongoing protest activity related to police executions. I want to start talking about the election during our Breakdown series because as we know, it's one of those areas that is ripe for disinformation, particularly the kind that we're concerned about in the Assembly program, which is state-backed, coordinated disinformation operations.**

***Brian, can you talk a little bit more in-depth about what you do at DHS on CISA?***

**BS:** Sure. I lead a small team. We're focused on what we call countering foreign influence, but, really, what we're trying to do is build national resilience to foreign influence activities. And so, for us, a lot of what we do is public education and public awareness, outreach to different communities, to provide resources that folks can use to better understand both the risk and then ways to mitigate the risk.

For us in particular, we're trying to reduce the amount that Americans engage with disinformation. And so, a lot of our products and information are focused on that. Also, specific to the election, we work a lot with state and local election officials to help them with content around the security of the election, so helping citizens understand how to vote, where to vote, how an absentee ballot works, things like that. We do that in support of state and local election officials.

Our two main areas are really trying to help folks understand what's going on around the 2020 election and then building broader, long term resilience to disinformation amongst the American people.

***OL: In terms of the contrast between what happened in 2016 and what we expect to observe this fall, what have we learned about state-backed disinformation operations since 2016? What were the big takeaways from your perspective?***

**BS:** Of course. Sure. We've actually learned a lot. I think a lot of what we draw from is, one, the Mueller report, and the indictments. There's a lot of detail and information about how the Russians acted and behaved, and what they did in 2016. The Senate Intel Committee reports have been a fantastic resource. And then, since 2016, the research community, in particular, has been extraordinary in terms of really diving deeply into what happened in 2016 and what we're seeing since then.

So, I think a few of the important things we've learned since 2016 from those reports is, one, we've got a better sense of both the sophistication and the reach of Russian efforts in 2016. It was really interesting for me to read about how the Russians had agents on the

ground in the United States trying to better understand our political environment, for example.

It was really interesting to learn and understand how they tried to set up and protest, where they would have both sides protesting against each other. It wasn't just on social media, but to bring things into the real world and to have people really acting and behaving a certain way, and trying to get conflict and conflict and conflict. So, those tactics were super interesting.

The other thing that was really interesting is really seeing how they were running it like a marketing or advertising campaign. They were A/B testing messaging. They were using data analytics to understand what narratives and messages were most effective, and then they were tailoring what they were doing based on that. And so, those two big things, from a tactical standpoint, and then, from a marketing/advertising/communications standpoint, was super fascinating.

For me, personally, the area that I've learned the most is really the psychology behind disinformation, why disinformation works and starting to see a lot of the research coming out about the psychology of disinformation, why disinformation works on humans, and Americans, why people jump into it.

We talk a lot about tech solutions to disinformation. For me, tech solutions are helpful, but the real problem is a human problem. How do we better understand the human aspects of disinformation? And then, how can we work to mitigate those sorts of things?

**OL:** ***Can you talk a little bit more in specific terms about what you've learned about the psychology of disinformation?***

**BS:** Sure. [The] first thing I learned about the psychology of disinformation is that there's not a lot of consensus in the research community about what works and what doesn't work, in terms of mitigating the risk. So, for us and for my job, we're trying to help people take steps to minimize the amount of engagement or sharing or liking or retweeting or whatnot that occurs, of disinformation and misinformation.

The research is good, but I haven't found where there's a strong consensus about the types of things that work and don't work. And so, that, of course, makes it a little bit challenging. There is some really good research about fact-checking and how fact-checking works or

doesn't work. In particular, repeating the false information is never a good thing. So, even if you're fact-checking something, not to share false information. I think that's really important.

The other area for us in particular that we're really focused on is the importance of pre-bunking. And so, the idea and the psychology basically says that once a thought is in your head, once you have an idea in your head, it's very difficult to dislodge that idea, even with factual information, even with new and improved information and better research.

And so, it's so critical to get accurate, reliable information out there first so that rather than responding to the disinformation, the disinformation is responding to the accurate information. The disinfo is trying to push to get information out of somebody's head. And so, how can we get out there and do that pre-bunk messaging around issues that we know are going to be critical to the 2020 election and things like that, where we know there's likely to be disinformation pushed?

**OL: I think that's exactly right. One of the other questions I had was related to what you mentioned earlier about protest activity, how IRA agents staged counterprotests on the same issue in the US. And, we are in such an interesting world in 2020, where they don't have to do any of that work at all.**

***Those protests are already going on. Are you seeing or is DHS seeing any attempts by state actors to use ongoing protest activity here for their own geopolitical aims?***

**BS:** It's been interesting about the current protests … The short answer is yes. But, what's been interesting about it is it's been mostly overt, open communications. I'm sure there's some covert activities going on, where they have their false accounts and things like that. But, if you just look at state-run media, if you just look at diplomatic communications, where the embassies are tweeting things out or posting messages, it's very overt communications, where they're trying to take advantage of the discord in the United States.

Again, the goal of nation-state actors is to reduce the strength of the United States, so they have a better chance to achieve their strategic goals. And so, anything they can do to undermine the legitimacy of the United States, undermine the legitimacy of democracy, they're going to take advantage of that. This is obviously a perfect opportunity for them to

do that. It's a legitimate, real issue here in the United States that we have to deal with, and those are the most effective ways to create fissures and divisions. It's just a reality, unfortunately.

**OL:** ***Have you seen any changes in how state actors are maybe seeding or planting disinformation online?***

**BS:** Sure. Absolutely. We've seen some changes. As the platforms and as governments have become more aggressive in terms of dealing with automated accounts and bots and inauthentic activity, the bad actors, of course, continue to change their tactics and their tools.

So, we've seen a few things, I think, that are important. One, we've seen new actors, both state and non-state actors, really take on the Russian playbook from 2016. So, the first thing that we're seeing is just a lot more players in the field. It's not just the Russians who are pushing it. It's a range of state actors.

And then, more importantly, I think, and more challenging, certainly from a government standpoint, is we have a lot of domestic actors that are taking the playbook from 2016 and leveraging it for their own purposes now. So, that's, I think, first and most important.

From a more tactical level, we've also seen a few different changes. State actors now are much more focused on amplifying, as we were just talking about, existing narratives that exist in the United States. In 2016, there was more where the state actors were creating narratives and then trying to amplify the narratives that they created. Now, what we're seeing more of is where they're just jumping on and getting behind narratives that are being pushed by American citizens. So, they don't have to create the content themselves. They just jump onto existing narratives, and disinformation is being pushed. So, that's one.

Two, we've seen more leveraging of proxies. And so, back a month or two ago, there was a great story that CNN did, using some really excellent research from a variety of different researchers, where they actually sent a reporter to Ghana, where Russians were leveraging a Ghana social media marketing company to do disinformation in the United States. And so, we're seeing a lot more of that, where they're trying to identify local proxies because it makes it much more difficult for the platforms in particular to identify inauthentic activity.

And so, we're seeing more of that. I don't think, as a government official, I'm allowed to promote a particular news agency. But, if you get a chance, that story and that research is really fascinating, to see how it's actually being done on the ground and how it actually works.

Another thing we're seeing a lot of is what we call disinformation as a service. This is where companies are essentially offering disinformation services. You can go hire somebody to run disinformation on your behalf. And so, again, it just opens up the playing field for the number of actors who can get involved and be involved in disinformation activities.

And then, of course, you're just seeing ramping of old becomes new, so forgeries, things like that. We've seen some, where rather than trying to subvert reporters, they're creating fake reporters and fake news sites to push articles and things like that. And then, you see a lot of leveraging of overt media and activities, and connecting state-run media with narratives and using a state-run media to amplify and things like that as well.

So, there's a lot going on. I think we'll see a lot of what we've seen in the past, but then you'll see some of these new items and some tweets and things like that, to try to make it more effective.

**OL: Yep. I know one challenge that came out of the Mueller investigation was that there's a pretty clear avenue for prosecuting state actors or non-US persons who participate in these operations, but not so much for US persons, American citizens.**

***Can you talk a little bit about how the government has responded to that difficulty since 2016?***

**BS:** Yeah. So, I mean, I think that's an important question. Foreign actors can break the law, and they can be investigated and hopefully prosecuted. Obviously, the prosecution can be difficult. For US citizens, there's First Amendment protections for speech and how we deal with that. So, it's a difficult topic.

I mean, there's a lot of incentives for folks to push and conduct disinformation operations, for their personal gain or political gain within the United States, and that creates a challenge. We can't investigate First Amendment protected speech. The FBI and DOJ can't

do anything about that, and DHS is certainly not getting involved in trying to do anything around domestic speech.

That is essentially bad actors taking advantage of our freedoms. American citizens, we can post up our opinions however we want, whenever we want, and foreign actors can come in and find the worst of those opinions or the most divisive of those opinions and amplify them. And so, it is definitely a particular challenge when domestic actors and participating and active in disinformation. I don't know that there's a good answer to that problem. Certainly not yet.

**OL:** ***Yeah. What do you see as the government's overall role in combating disinformation?***

**BS:** That is the $64,000 question, right? That's a good question. I think the first thing … And, this is something I grapple with regularly. It was something when I was up in the fellowship that I talked to my fellow fellows about quite a bit. That's going to make for great podcasting right there, fellow fellows …

**OL: Fellow fellows. I'm writing that down.**

**BS:** I think it's a really difficult question. It's not just a difficult question about what's the government's role? I think we have to be talking about what the platforms' role is, what tech companies' role is, what civil society's role is, and what the individual's role is, in dealing with combating disinformation.

So, from the government side, I think what we're doing now is essentially leveraging the authorities and what we can legally do. So, we have the intelligence community helping to understand the threat, identifying bad actors, doing the things that the intelligence community does, and does very well.

And then, we have our law enforcement agencies, the FBI, the DOJ. They're investigating when the law is violated. When a law is broken, they're investigating, indicting, prosecuting the bad actors. That's great, and that's a piece of it.

And then, we have to build what DHS is doing with trying to build public resilience. We're trying to help the American people understand the role that they play and the steps that they can take.

And then, of course, at a broader level, particularly for state actors, we need to establish deterrence measures. I believe the State Department and the National Security Council interagency more broadly is working on how can we deter state actors from trying to interfere in what we're doing? And so, I think those are the things that government can do now, and that's what we're trying to do now within the authorities we have.

The question is, we have people calling for more monitoring of speech on platforms. We have to tell the platforms that this is a lie, and they need to take it down. Or, we're asking the platforms to do that. And so, that gets into protected speech and First Amendment rights. I think those are super difficult challenging questions we have to deal with. It's things, as government, we deal with every day, not only the free speech issues and First Amendment protections, but privacy issues and those sorts of things.

As you know, attributing an actor on social media is difficult. Anonymity is the thing on social media for a lot of these platforms. It's very difficult to identify and attribute who's saying something. And so, if you don't know who's saying something, it could be an American citizen. How do you deal with that? If you know it's a foreign actor, it's a little different approach to it. From a government standpoint, it opens up some different avenues for us. But, if you don't know or if it's potentially an American citizen, how do you deal with that differently?

My view is I think we need a broader national discussion on roles and responsibilities. What's the government's role? What's the platforms' role? What's the tech companies' role? What are the individual citizens' role? How can we leverage civil society in this space? I don't know that we've gotten there yet, but I think that conversation needs to occur.

And so, the government right now, I think we're leveraging our authorities. I think, certainly, from a DHS standpoint, we try to push as much we can. But, we're also super cautious. I don't know how you can be aggressively cautious, but I think that's generally our approach because we're very, very concerned about privacy and First Amendment protections and things like that. And, I know that our interagency partners feel the same way as well.